REMARKS

The Office Action dated September 12, 2005 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 15, and 25 have been amended to more particularly point out and distinctly claim the subject matter of the invention. No new matter has been added and no new issues are raised which require further consideration or search. Claims 4, 20, and 28 have been cancelled without prejudice. Therefore, claims 1-3, 5-19, 21-27, and 29-33 are currently pending in the application and are respectfully submitted for consideration.

In the Office Action, claims 1-4, 6-16, and 18-24 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tello (U.S. Patent No. 6,463,537) in view of Angelo (U.S. Patent No. 6,370,649). The Office Action took the position that Tello discloses all of the elements of the claims, with the exception of a host configured to receive a guess passcode from a manufacturer. The Office Action then relies upon Angelo as allegedly curing this deficiency in Tello. The rejection is respectfully traversed for the reasons which follow.

Claim 1, upon which claims 2-14 are dependent, recites an apparatus for enabling functionality of a component. The apparatus includes a random number generating module for generating a random number, a hash function module in communication with the random number generating module, a host in communication with the random

number generating module, at least one memory in communication with the host, an encryption module in communication with the memory, and a comparing device in communication with the encryption module and the hash function module. The comparing device compares a first bit string to a second bit string in order to generate a function enable output for the component. The at least one memory further comprises a guess register in communication with the host and the encryption module, the guess register being configured to receive a guess passcode from the host, and a public key module in communication with the encryption module, the public key module being configured to store a public key therein. The host is configured to receive a guess passcode from the manufacturer of the component.

Claim 15, upon which claims 16-24 are dependent, recites a component for selectively enabling a functionality of an electronic device. The component includes a means for generating a random bit string, a hash function module in communication with the means for generating, a means for acquiring a guess passcode in communication with the means for generating, an encryption module in communication with the means for acquiring, and a comparing device in communication with the encryption module and the hash function module. The comparing device has an output for transmitting a functionality enable signal therefrom. The encryption module further comprises a public key encryption module, and a public key module in communication with the public key encryption module. The public key encryption module is configured to receive a public key from the public key module and a guess passcode from the means for acquiring, and

generate a ciphertext bit string therefrom. The means for acquiring the guess passcode is configured to acquire the guess passcode from the manufacturer of the electronic device.

The prior art has failed to produce enablement methods that are effective against reasonably sophisticated attackers. The claimed invention resolves the limitations of the prior art by providing, in one example, a cryptographic method wherein the secure portions of the method are implemented in electronic or computer products. More specifically, embodiments of the claimed invention implement cryptographic functions for enabling functionality of electronic/computer related components, wherein the relevant secure key related information is contained within computer hardware in a non-volatile memory device and not within a purely software driven configuration. The claimed invention also provides the ability to conduct secure functionality enablement on electronic/computer related components, wherein a public key for enabling the component is contained onboard and utilized in conjunction with a randomly generated component identifier in order to selectively enable additional functionality of the component.

As will be discussed below, Tello and Angelo, whether viewed singly or combined, fail to disclose or suggest the elements of the claims, and therefore fails to provide the advantages discussed above.

Tello discloses a modified computer motherboard security and identification system. More specifically, Tello discloses a modified motherboard with a microprocessor based security engine, enabling and disabling circuits, memory buffer

circuits, modified BIOS, modified DDL, and a smart card reader and smart cards. Upon startup of the computer, the modified BIOS takes control and allows the security engine microprocessor to look for and read from a smart card in the smart card reader that is connected to the security engine microprocessor. A unique hash number is placed in the smart card during the initial set up of the security system and a complimentary hash number is assigned to the security engine memory. During startup, a software program in the flash memory of the security engine compares the hash numbers in the smart card and the computer. If these two hash numbers are compliments, the boot up procedure is allowed to continue and access to the computer is allowed.

Angelo discloses a computer system with a self-modifying "fail-safe" password system that allows a manufacturer to securely supply a single-use password to users who lose or misplace a system password. The fail-safe password system utilizes a fail-safe counter, an encryption/decryption algorithm, a manufacturer's public key, and a secure non-volatile memory space. Each time a fail-safe password is entered into the computer system, an application decrypts the fail-safe password and compares the resulting value, which is a hash code, to an internal hash value and increments the fail-safe counter or modifies the seed value when the hashes match. When the fail-safe counter is incremented, the previous fail-safe password is no longer valid.

Applicants respectfully submit that the combination of Tello and Angelo fails to disclose or suggest all of the elements of claims 1 and 15. For example, Tello and Angelo, whether viewed alone or combined, fail to disclose or suggest that the at least

one memory comprises a guess register in communication with the host and the encryption module, the guess register being configured to receive a guess passcode from the host, and a public key module in communication with the encryption module, the public key module being configured to store a public key therein, as recited in claim 1. Similarly, Tello and Angelo fail to disclose or suggest that the encryption module comprises a public key encryption module, and a public key module in communication with the public key encryption module, wherein the public key encryption module is configured to receive a public key from the public key module and a guess passcode from the means for acquiring, and generate a ciphertext bit string therefrom, as recited in claim 15.

Therefore, as recited in claims 1 and 15 and supported in the specification, the present invention provides, in one embodiment, a novel apparatus and method for selectively and securely enabling additional functionality of an electronic component. More specifically, according to one aspect of the invention, a host 18 is provided and is in communication with memory 28, which contains an identification number that may correspond to the component to be enabled by the public key encryption device 33. Memory 28 communicates the component identification number to hash function module 29 as a pre-image input. Hash function module 29 processes the pre-image input and generates a hash value at an output of hash function module 29 which is transmitted to the second input 20b of comparator 20. Host 18 also obtains a guess passcode that is transmitted to guess register 19. The passcode is then transmitted as clear text to public

key encryption module 35. Public key module 34, which contains the public key for the device therein, transmits a public key to public key encryption module 35. As such, public key encryption module receives both the guess passcode and the public key as clear text inputs. These two inputs are processed/encrypted by public key encryption module 35 to generate cipher text at the output of public key encryption module 35. This cipher text is transmitted to the first input 20a of comparator 20. Comparator 20 then compares the cipher text received from public key encryption module 35 representing the guess passcode to the hash value generated by hash function module 29 representing the identification number of the component. If the two values match, then an enable signal is output from comparator 20 (Specification, page 23, line 14 – page 24, line 21, see Figure 3).

Applicants respectfully submit that the cited prior art references of Tello and Angelo fail to disclose or suggest the configuration of the present invention, as discussed above. Tello only discloses that a public encryption algorithm is embedded in the smart card ROM and a block of data is encrypted by the smart card before it is sent to the security engine. Further, when the registers are read from the smart card to determine the type of card inserted, an encrypted code number is read from the register of the inserted smart card and decrypted by the security engine microprocessor using the public encryption key 475 (Tello, Column 24, lines 15-20 and 46-50). The present claims, on the other hand, recite that the public key encryption module is in communication with both the guess register and the public key module. In addition, the public key encryption

module receives both the guess passcode from the guess register and a public key from the public key module. The public key encryption module then encrypts the two inputs in order to generate a cipher text (Specification, page 24, lines 1-10 and Figure 3). Tello does not disclose receiving a guess passcode and public key and then processing these two inputs to produce a cipher text. Rather, Tello merely discloses reading an encrypted code from the register of the smart card and **decrypting** the code using a public encryption key (Tello, Column 24, lines 46-50). Therefore, Tello fails to disclose or suggest at least this element of claims 1 and 15. Angelo also fails to disclose or suggest such a limitation.

Furthermore, Applicants respectfully submit that Tello and Angelo do not disclose or suggest a hash function module in communication with a random number generating module, as recited in present claims 1 and 15. The Office Action cites Tello as allegedly disclosing this limitation of the claims. However, Tello only discloses that an algorithm generates hash numbers H1, H2, H3 which are then encrypted to generate H1', H2', H3' (Tello, Column 8, lines 10-16). Tello does not disclose or suggest that the algorithm for generating the hash numbers is in communication with a random number generating module. In the response to arguments section of the Office Action, it is alleged that the encrypted hash numbers constitute a random generating module in communication with the hash function module. Applicants respectfully disagree. According to the present invention, the generated random number is transmitted to the input of hash function module 29 as pre-image information (Specification, page 26, lines 10-13). Consequently,

the hash function module receives a random number as an input and generates a hash value at the output of the hash function module 29 (Specification, page 27, lines 1-5). As such, the encrypted hash numbers of Tello cannot be considered to correspond to the random number generated in the present invention which is utilized to produce a hash value. In addition, Angelo also does not disclose or suggest that a hash function module is in communication with a random number generating module. Therefore, Tello and Angelo, whether viewed individually or combined, fail to disclose or suggest at least this element of claims 1 and 15.

For at least the reasons discussed above, Applicants respectfully assert that claims 1 and 15 recite limitations that are neither disclosed nor suggested by the cited prior art. Thus, Applicants respectfully request that the rejection of claims 1 and 15 be withdrawn.

Applicants note that claims 2-14 and 16-24 are dependent upon claims 1 and 15, respectively. Consequently, claims 2-14 and 16-24 should be allowed for at least their dependence upon claims 1 and 15, and for the specific limitations recited therein.

Claims 5 and 17 were rejected under 35 U.S.C. §103(a) as being unpatentable over Tello in view of Angelo and further in view of Crouch (U.S. Patent No. 5,383,143). The Office Action took the position that Tello and Angelo disclose all of the elements of claims 5 and 17, with the exception of a linear feedback shift register, a NAND gate, and at least one inverter in communication with the linear feedback shift register and NAND gate. The Office Action then relies upon Crouch as allegedly curing these deficiencies in

Tello and Angelo. The above rejection is respectfully traversed for the reasons which follow.

Tello and Angelo are discussed above. Crouch discloses a self re-seeding linear feedback shift register data processing system for generating a pseudo-random test bit stream. The data processing system 10 has a test controller 12 with a pattern generator 18 for receiving a seed value and generating many pseudo-random values from the seed value. A re-seed and compare circuit 22 monitors the pattern generator 12 and determines when the seed value repeats in the pseudo-random number sequence generated by the generator 18. Once the compare circuit 22 determines that the seed value has repeated, the control circuit 20 allows the generator 18 to clock once more and latches a new seed value into the circuit 22.

Applicants note that claims 5 and 17 are dependent upon claims 1 and 15, respectively. Further, as discussed above, the combination of Tello and Angelo fails to disclose or suggest all of the elements of claims 1 and 15. Additionally, Crouch fails to cure those deficiencies in Tello and Angelo. As such, claims 5 and 17 should be allowed for at least their dependence upon claims 1 and 15, and for the specific limitations recited therein.

Claims 25-33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Davis (U.S. Patent No. 5,577,121) in view of Tello and further in view of Angelo. The Office Action took the position that Davis discloses all of the elements of the claims, with the exception of the second bit string being encrypted using a public key and receiving

the second bit string from a manufacturer of the electronic component. The Office Action then relies upon Tello and Angelo as allegedly curing this deficiency in Davis. The rejection is respectfully traversed for the reasons which follow.

Claim 25, upon which claims 26-33 are dependent, recites a method for enabling functionality of an electronic component. The method includes the steps of generating a random number, calculating a first bit string from the random number, determining a second bit string corresponding to the random number, encrypting the second bit string with a public key to generate a third bit string, comparing the third bit string to the first bit string to determine a match, and outputting a function enable signal in accordance with the comparison. The encrypting step further comprises the steps of receiving a guess passcode from a host, receiving a public key, and encrypting the guess passcode and the public key to generate a ciphertext bit string. The step of determining the second bit string comprises receiving the second bit string from the manufacturer of the electronic component.

Tello and Angelo are discussed above. Davis discloses a transaction system for integrated circuit cards, and more specifically it discloses a method of conducting a transaction between an integrated circuit (IC) card and a transaction terminal which includes a security module. The method includes establishing communication between the terminal and the IC card and separately generating a session key in the IC card using data stored in the IC card and a code associated with the particular IC card and in the security module using data stored in the security module and the code associated with the

particular IC card. The session key generated by the IC card is used to encrypt data using an encryption algorithm to obtain a first result and the session key generated by the security module is used to encrypt the same data using the same encryption algorithm to obtain a second result. The first and second results are compared and the terminal will conduct the transaction only if the comparison establishes that the first result and the second result are identical.

Applicants respectfully submit that the combination of Davis, Tello and Angelo fails to disclose or suggest all of the elements of claim 25. Specifically, Applicants respectfully submit that Davis, Tello and Angelo, whether considered singly or combined, fail to disclose or suggest that the encrypting step comprises receiving a guess passcode from a host, receiving a public key, and encrypting the guess passcode and the public key to generate a ciphertext bit string, as recited in present claim 25. As discussed above, the present invention provides that the public key encryption module is in communication with both the guess register and the public key module. The public key encryption module receives both the guess passcode from the guess register and a public key from the public key module. The public key encryption module then encrypts the guess passcode and the public key in order to generate a cipher text (Specification, page 24, lines 1-10 and Figure 3).

Davis, on the other hand, only discloses that the security module retrieves from its memory a control password key and encrypts the SVC serial number with the control password key using the DES algorithm to produce a derived password (Davis. Column

13, lines 56-60). Therefore, Davis teaches that the control password key is stored in the memory of the security module and is used to encrypt the SVC serial number. Davis does not disclose or suggest a public key is received from a public key module, while a guess passcode is received from a guess register. Furthermore, Davis does not disclose or suggest encrypting the guess passcode **and** the public key to generate a ciphertext bit string. Rather, Davis discloses using the control password key to encrypt the SVC serial number. Therefore, Davis fails to disclose or suggest at least this limitation of claim 25. Furthermore, Tello and Angelo as discussed above, also fail to disclose or suggest such a limitation.

In addition, Applicants respectfully submit that Davis, Tello, and Angelo all fail to disclose or suggest determining a second bit string corresponding to the random number, as recited in claim 25. The Office Action cites Davis as allegedly disclosing this element of the claim. Applicants submit that Davis does not determine a second bit string which corresponds to the random number. Rather, according to Davis, the security module generates a random number and sends it to the SVC. The SVC encrypts the random number with the SVC session key. The security module encrypts the random number with the security module session key (Davis, Column 13, lines 6-52). Therefore, Davis only discloses generating a random number which is then encrypted by the SVC and security module. Davis does not disclose that a second bit string corresponding to the random number is determined. In addition, Tello and Angelo do not disclose or suggest such a limitation.

For at least the reasons discussed above, Applicants respectfully submit that the combination of Davis, Tello, and Angelo fails to disclose or suggest all of the elements of claim 25. As such, Applicants respectfully request that the rejection of claim 25 be withdrawn.

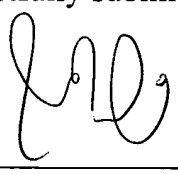
It is also respectfully submitted that claims 26-33 depend from claim 25 and therefore should be allowed for at least their dependence on claim 25, and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited prior art references fail to disclose or suggest critical and important elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unobvious. It is therefore requested that all of claims 1-3, 5-19, 21-27, and 29-33 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MSA:jf